REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are pending in the application. The Examiner additionally stated that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are rejected. By this communication, claims 1, 6, 11-13, 56, 29, and 66-67 are amended. Hence, claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-6, 11-12, 24-25, 27, 56-60, 66, and 79-83 under 35 U.S.C. 103(a) as being unpatentable over Kessler et al., U.S. Patent 6,789,147 (hereinafter, Kessler) in view of Best, U.S. Patent 4,278,837, (hereinafter, Best). Applicant respectfully traverses the Examiner's rejections.

Regarding claim 1, the Examiner noted that Kessler discloses a processor apparatus for performing a cryptographic operation comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a processor (col. 4, line 59-col. 5, line 36), said instruction flow comprising an instruction, configured to direct said processor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the

cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 - col. 6, line 10); and a cryptography unit, disposed within execution logic in said processor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55); and an integer unit, disposed within execution logic in said processor and coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation (col. 9, lines 15-20).

The Examiner conceded that the processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred narrow definition of "microprocessor" established in the specification. However, the Examiner asserted that Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 & 18). The Examiner also noted that Best clearly discloses wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The Examiner concluded that the claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the cryptographic unit of Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

The Examiner noted that Best places no limitations as to the specific architecture employed by the prior art microprocessor functional unit of the hybrid microprocessor; nevertheless, the Examiner took Official Notice that, given the ubiquity of the x86 architecture as well as past instances where the general technique of integrating a coprocessor into an x86-based microprocessor had previously been practiced in the art,

that it would have been immediately obvious to use an x86-compatible microprocessor as the prior art microprocessor unit of the Best invention [in view of Kessler]. Additionally, pursuant to MPEP 2144.03, see the Examiner referred Applicant to a Wikipedia reference entered into the record on 6/4/08: page 2, "History" and "Design"; as well as page 4, 3rd paragraph.

Regarding claim 56, the Examiner noted that Kessler discloses an apparatus for performing cryptographic operations, comprising: fetch logic, disposed within a processor, configured to fetch an instruction flow from memory for execution by a processor by said processor (col. 4, line 59 - col. 5, line 36), said instruction flow comprising an instruction, configured to direct said processor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 - col. 6, line 10); translation logic, disposed within said processor, configured to translate said cryptographic instructions into associated micro instructions that specify sub operations required to accomplish said one of the cryptographic operation (e.g. col. 8, lines 11-16); and a cryptography unit, disposed within execution logic in said processor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55).

The Examiner stated that the processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred definition of "microprocessor" established in the specification. However, the Examiner stated that Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional

microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 &18) and, additionally, Best clearly discloses wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The Examiner concluded that the claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the cryptographic unit of Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

The Examiner noted that Best places no limitations as to the specific architecture employed by the prior art microprocessor functional unit of the hybrid microprocessor; nevertheless, the Examiner took Official Notice that, given the ubiquity of the x86 architecture as well as past instances where the general technique of integrating a coprocessor into an x86-based microprocessor had previously been practiced in the art, that it would have been immediately obvious to use an x86-compatible microprocessor as the prior art microprocessor unit of the Best invention [in view of Kessler]. Additionally, pursuant to MPEP 2144.03, see the Examiner referred Applicant to a Wikipedia reference entered into the record on 6/4/08: page 2, "History" and "Design"; as well as page 4, 3rd paragraph.

Responsive to previous arguments submitted by Applicant, the Examiner noted for the record that Applicant appears to believe that there remains a point of contention regarding the appropriate scope of the claim term "microprocessor" (see the amendment of 2/25/09, page 21, 2nd paragraph), when to the Examiner's mind this point had been settled in the Applicant's favor in the Non-Final Office Action of 6/4/08 (see pages 2-3, paragraph #4), noting that Applicant had, at that time, correctly pointed out that the instant specification provides a context-specific definition of the term "microprocessor" in a manner as to exclude "coprocessors"; since claim limitations are read in light of the instant specification, thus Examiner had henceforth interpreted the claim term "microprocessor" using Applicant's preferred definition and that this is precisely the

reason why the Best reference was subsequently cited in the rejections, as Best where cited discloses that as an alternative to employing a separate microprocessor and cryptographic coprocessor, one could instead incorporate both as functional units within a single hybrid microprocessor, fully capable of both executing software and performing cryptographic operations (most clearly illustrated at col. 19, lines 20-35). As to amending the independent claims to stipulate wherein the microprocessor is x86-compatible, while Examiner admitted that the Best reference in particular does not explicitly state that the prior-art microprocessor to be combined with the cryptographic unit of Best's invention is an x86 processor, nevertheless the Examiner insisted that he has already entered into the record ample evidence that the x86 processor architecture was sufficiently well-known among those of ordinary skill in the art as to make this limitation obvious. Specifically, it was noted that the Wikipedia reference entered into the record on 6/4/08 teaches that not only was the x86 architecture "the most popular CPU architecture ever" (page 2, "History") but that for decades people of ordinary skill in the art have recognized the need to augment the functionality of x86 microprocessors (page 2, "Design, 1st paragraph), including inter alia by integrating functionality formerly reserved for a separate coprocessor as a functional unit of the next generation x86 microprocessor (Wikipedia, page 4, "The Intel 80387 math co-processor was integrated into the next CPU in the series, the Intel 80486", et al.). Thus, the Examiner submitted that it would have been immediately obvious to one of ordinary skill in the art by the time of the instant invention to use an x86 microprocessor as the prior art microprocessor functional unit of Best's hybrid microprocessor, for at least two reasons: first, given the ubiquity and popularity of the x86 architecture by the time of the instant invention, one of ordinary skill in the art would have had good reason to use a processor compatible with "the most popular CPU architecture ever" as Best's prior art microprocessor, as this would have been the result not of innovation but of ordinary skill and common sense; and second, Best's technique of incorporating coprocessor functionality into a microprocessor had clearly long since been part of the capabilities of one of ordinary skill in the art, given that this technique had already been practiced previously in the history of the x86 architecture. See KSR v. Teleflex, 550 U.S. 398, 82 USPQ2d at 1395-1397 (2007).

Examiner also wishes to remind the Applicant for future reference that the specific features of the x86 architecture that Applicant has appealed to in order to distinguish the claimed invention from the prior art (e.g. MMX, SSE, etc.) are not present in the claims and although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Nevertheless, the Examiner submitted that even if such features had been claimed, said features would have been inherent to all x86 processors that would have been available to one of ordinary skill in the art by the time of the instant invention, as earlier x86 processors lacking one or more of said features were known to be obsolete or obsolescent by then (see the enclosed "PC Hardware in a Nutshell, 2nd Edition" reference, particularly pages 8-10).

Applicant also respectfully submits that it is his sincere desire to forward this case through the Office in all candor and good faith, and thus he has amended claims 1 and 56 specifically to recite, among other features and limitations, that the cryptographic instruction with is executed by the microprocessor is “atomic.” Such a limitation is very well known in the art and is furthermore clearly taught in the instant specification.

Applicant accepts most of the Examiner’s arguments summarized above regarding the ubiquitous nature of the x86 architecture and the obvious desire within the community to incorporate features (i.e., floating point processing) into an x86-compatible microprocessor which would otherwise be performed by a coprocessor. Certainly, Kessler lays out the problems associated with performing security functions in a processor, and Best alludes to how it would be desirable to provide a hybrid circuit that includes a deciphering circuit coupled to a microprocessor.

But Applicant responds that there are several problems when combining the teachings of Best and Kessler that preclude one skilled in the art from envisioning the limitations noted in the independent claims. First, it is noted that such a “desire” to incorporate features into a microprocessor, as is suggested by the Examiner by using citations from Best, would most likely have yielded some microprocessor having cryptographic functionality, particularly an x86-compatible microprocessor, since the Best reference has

been in the public domain for nearly 30 years. Yet, prior to the present invention, no microprocessor has been developed having the capabilities recited in the independent claims. This leads one skilled in the art, and it is respectfully submitted by Applicant, to question the combination of Kessler and Best.

More specifically, the cryptographic "operation" performed by the Best invention is exclusively deciphering of a program stored in memory, for execution by the microprocessor. Thus, Best does not teach an "instruction" that directs a cryptographic operation to be executed by a microprocessor, but rather teaches instructions that direct non-cryptographic operations to be performed by the microprocessor, where the instructions must be deciphered first prior to execution. Applicant thus submits that the sequential nature of these to operations (i.e., decipher then execute) lends itself very easily to the hybrid circuit suggested by Best because these operations can be independently executed as long as they are performed in the proper sequence. But it is argued that this is not the same as fetching an instruction from memory that directs the microprocessor to perform a cryptographic operation, and then having the microprocessor to perform the cryptographic operation itself, such as encryption or decryption of data stored in memory.

There is a significant hurdle that has precluded any in the art from fielding a cryptographic instruction and a commensurate microprocessor (x86-compatible or otherwise) capable of executing the cryptographic instruction. Stated succinctly, the problem is atomicity. That is, in order to perform, say, an AES block encryption operation, one skilled in the art will appreciate that literally thousands of sub-operations must be performed in a manner that is entirely transparent to the operating system and must function reliably in the presence of interrupts. These operations and their difficulty are noted in the instant specification in paragraphs associated with FIGURES 1 and 2, and it is respectfully submitted that the problems associated with provided for atomic execution of a cryptographic instruction are why heretofore cryptographic operations have been relegated to program subroutines (e.g., Kessler) and coprocessors. It has been too difficult to provide for atomicity of these complicated operations that require numerous processor resources (i.e., integer unit).

Accordingly, Applicant has amended the claims to specifically recited that this instruction is "atomic." Applicant also respectfully asserts that the term "atomic" is very well known to those skilled in the microprocessor arts, but may not be well known to those who deal primarily with cryptographic devices such as those taught by Kessler and Best. However, it is noted that a large portion of the specification is devoted to teaching how such an atomic instruction is executed in the presence of operating system considerations and interrupts.

Applicant also respectfully submits that neither Kessler nor Best teach or suggest an atomic cryptographic instruction and a microprocessor capable of executing such. Accordingly, their combination does not yield this limitation either and it is respectfully submitted that the rejections of claims 1 and 56 are overcome.

In view of the above points, Applicant respectfully requests that the rejections of claims 1 and 56 be withdrawn.

In addition, Applicant notes that the addition of the limitation "atomic" to the independent claims is a good faith attempt to forward this application through the Office and furthermore submits that no further elaboration is needed to convey to one skilled the what is meant by "atomic" for such a term is well known in the microprocessor arts. However, it is also noted that the primary considerations for execution of an atomic instruction (e.g., operating system transparency) are additionally taught within the instant specification, and the Examiner is strongly encouraged to contact the undersigned should he feel a need to further define the term "atomic" within the claims.

With respect to claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83, these claims depend from claims 1 and 56 as appropriate, and add further limitations that are neither anticipated nor made obvious by Kessler, Best, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83.

The Examiner rejected claims 7-10 and 61-64 under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Best, as noted above, and further in view of "Applied Cryptography, 2nd Edition."

Applicant respectfully traverses the Examiner's rejections and notes that claims 7-10 and 61-64, depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 7-10 and 61-64.

The Examiner additionally rejected claims 13-22 and 67-76 under 35 U.S.C. 103(a) as being unpatentable over Kessler and further in view of Johns-Vano et al. (U.S. Patent 6,026,490). Applicant respectfully traverses and notes that claims 13-22 and 67-76 depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 13-22 and 67-76.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

08/23/2009

Date: _____